

IN THE CLAIMS:

This listing of the claims replaces all prior versions and listings of the claims. Please add claims 24 and 25 and amend claims 7, 10, 12, 13, 22 and 23 as follows:

1 Claim 1. (original) A data storage device for an information
2 processing device, the data storage device comprising:

3 an encryption circuit for encrypting desired data and personal
4 identification information by use of an encryption key created out of a
5 given piece of the personal identification information;

6 a recording medium for recording the data and the personal
7 identification information encrypted by the encryption circuit; and

8 a control unit for executing user verification by use of the
9 encrypted personal identification information stored in the recording
10 medium.

1 Claim 2. (original) The data storage device according to claim
2 1,

3 wherein the encryption circuit encrypts the encryption key by use
4 of a different encryption key, and

5 the recording medium records the encryption key encrypted by use
6 of the different encryption key.

1 Claim 3. (original) The data storage device according to claim
2 1,

3 wherein the recording medium includes a special storage area
4 which is inaccessible in normal use, and

5 the recording medium records the encryption key in the special
6 storage area.

1 Claim 4. (original) The data storage device according to claim
2 1,

3 wherein the encryption circuit creates a plurality of encryption
4 keys out of a plurality of personal identification information and
5 controls the user identification and the data encryption depending on
6 each of the plurality of encryption keys, and

7 the recording medium manages the storage areas in accordance with
8 the plurality of keys, and records the encrypted data in the respective
9 storage areas by use of the corresponding encryption keys.

1 Claim 5. (original) A data storage device for an information
2 processing device, the data storage device comprising:

3 an encryption circuit for encrypting desired data by use of a
4 first encryption key and for encrypting the first encryption key and
5 personal identification information by use of a second encryption key
6 created out of a given piece of the personal identification
7 information;

8 a recording medium for recording the data encrypted by use of the
9 first encryption key, the first encryption key encrypted by use of the
10 second encryption key, and the personal identification information
11 encrypted by use of the second key; and

12 a control unit for executing user verification by use of the
13 encrypted personal identification information stored in the recording
14 medium.

1 Claim 6. (original) The data storage device according to claim
2 5,

3 wherein the encryption circuit decrypts the encrypted first
4 encryption key being read out of the recording medium by use of the
5 second encryption key, and executes any of encryption and decryption of
6 the desired data by use of the decrypted first encryption key.

1 Claim 7. (currently amended) A hard disk device comprising:

2 a magnetic disk being a recording medium;

3 a read-and-write mechanism for writing and reading data in and
4 out of the magnetic disk; and

5 a control mechanism having an encryption function for encrypting
6 data to be written in the magnetic disk and for decrypting the
7 encrypted data to be read out of the magnetic disk, the control
8 mechanism for controlling reading and writing the data by the reading-
9 and-writing mechanism,

10 wherein the control mechanism executes encryption of the data to
11 be written in the magnetic disk for each unit of writing and reading

12 data in and out of a storage area of the magnetic disk upon processing
13 of writing the data in the magnetic disk, in response to turning on and
14 off of the encryption mechanism, and

15 wherein the encryption function of the control mechanism encrypts
16 personal identification information by use of an encryption key created
17 out of a given piece of the personal identification information.

1 Claim 8. (original) The hard disk device according to claim 7,
2 wherein the control mechanism judges as to whether the data are
3 encrypted or not upon reading the data out of the storage medium, and
4 further decrypts the data when the data are encrypted.

1 Claim 9. (original) The hard disk device according to claim 7,
2 wherein the control mechanism decrypts the read-out data when the
3 data read out of the recording medium are encrypted, and
4 the control mechanism encrypts and writes the data in the
5 recording medium when the encryption function is turned on.

1 Claim 10. (currently amended) The hard disk device according to
2 claim 7,

3 wherein the encryption function of the control mechanism ~~includes~~
4 ~~an encryption function for encrypting~~ encrypts desired data ~~and~~
5 ~~personal identification information~~ by use of ~~an~~ the encryption key
6 created out of a given piece of the personal identification
7 information, and

8 the control mechanism executes user verification by use of the
9 encrypted personal identification information.

1 Claim 11. (original) The hard disk device according to claim 10,
2 wherein the encryption function of the control mechanism creates
3 a plurality of encryption keys out of a plurality of personal
4 identification information and controls the user identification and the
5 data encryption depending on each of the plurality of encryption keys,
6 and

7 the magnetic disk manages storage areas in accordance with the
8 plurality of keys, and records the encrypted data in the respective
9 storage areas by use of the corresponding encryption keys.

1 Claim 12. (currently amended) The hard disk device according to
2 claim 7,

3 wherein the encryption function of the control mechanism ~~includes~~
4 ~~an encryption function for encrypting~~ encrypts desired data by use of a
5 first encryption key and ~~for encrypting~~ encrypts the first encryption
6 key and ~~personal identification information~~ by use of a ~~second~~ the
7 encryption key created out of a given piece of the personal
8 identification information, and
9 the control mechanism executes user verification by use of the
10 encrypted personal identification information.

1 Claim 13. (currently amended) An information processing device
2 comprising:

3 an operation control unit for executing various operation
4 processing; and

5 a data storage device for storing data to be processed by the
6 operation control unit,

7 wherein the data storage device includes an encryption function
8 for encrypting desired data by use of a data encryption key and for
9 encrypting personal identification information by use of ~~an~~ a
10 verification encryption key created out of a given piece of the
11 personal identification information, and

12 the data storage device executes user verification by use of the
13 encrypted personal identification information.

1 Claim 14. (original) The information processing device according
2 to claim 13,

3 wherein the data encryption key and the verification encryption
4 are mutually identical.

1 Claim 15. (original) The information processing device according
2 to claim 13,

3 wherein the data storage device encrypts the data encryption key
4 by use of a different encryption key and saves the encrypted data
5 encryption key.

1 Claim 16. (original) The information processing device according
2 to claim 15,

3 wherein the data storage device encrypts the data encryption key
4 by use of the verification encryption key as the different encryption
5 key.

1 Claim 17. (original) A data processing method for a data storage
2 device for executing data writing and reading in and out of a recording
3 medium of a data storage device, the data processing method for a data
4 storage device comprising the steps of:

5 creating an encryption key out of a given piece of personal
6 identification information;

7 encrypting the personal identification information by use of the
8 encryption key and thereby recording the encrypted personal
9 identification information in the recording medium as verification
10 data;

11 executing user verification based on the verification data
12 recorded in the recording medium; and

13 executing any of encrypting write data transmitted from a host
14 system by use of the encryption key and thereby recording the encrypted
15 write data in the recording medium, and, decrypting the data read out
16 of the recording medium by use of the encryption key and thereby
17 transmitting the decrypted data to the host system.

1 Claim 18. (original) The data processing method for a data
2 storage device according to claim 17, further comprising the steps of:

3 encrypting the encryption key by use of a different encryption
4 key and thereby recording the encrypted encryption key in the recording
5 medium; and

6 decrypting the encrypted encryption key by use of the different
7 encryption key and thereby decrypting the data read out of the
8 recording medium by use of the decrypted encryption key.

1 Claim 19. (original) A data processing method for a data storage
2 device for executing data writing and reading in and out of a recording
3 medium of a data storage device, the data processing method for a data
4 storage device comprising the steps of:

5 creating a verification encryption key out of a given piece of
6 personal identification information;

7 encrypting the personal identification information by use of the
8 verification encryption key and recording the encrypted personal
9 identification information in the recording medium as verification
10 data, and further encrypting a data encryption key by use of the
11 verification encryption key and thereby recording the encrypted data
12 encryption key in the recording medium;

13 executing user verification based on the verification data
14 recorded in the recording medium;

15 decrypting the data encryption key recorded in the recording
16 medium by use of the verification encryption key; and

17 executing any of encrypting write data transmitted from a host
18 system by use of the decrypted data encryption key and thereby
19 recording the encrypted write data in the recording medium, and
20 decrypting the data read out of the recording medium by use of the data
21 encryption key and thereby transmitting the decrypted data to the host
22 system.

1 Claim 20. (original) The data processing method for a data
2 storage device according to claim 19, further comprising the step of:

3 decrypting the encrypted data encryption key recorded in the
4 recording medium along with a change in the personal identification
5 information by use of the verification encryption key created out of
6 the personal identification information prior to the change, and then
7 encrypting the data encryption key again by use of the verification
8 encryption key created out of the personal identification information
9 after the change and thereby storing the data encryption key in the
10 recording medium.

1 Claim 21. (original) The data processing method for a data
2 storage device according to claim 19, further comprising the step of:

3 decrypting the encrypted data encryption key recorded in the
4 recording medium upon disabling encryption of the data recorded in the
5 recording medium by use of the verification encryption key created out
6 of the personal identification information prior to a change and
7 thereby storing the decrypted data encryption key in the recording
8 medium.

1 Claim 22. (currently amended) A program stored in computer
2 readable memory for controlling a computer to control data writing and
3 reading in and out of a magnetic disk, the program causing the computer
4 to execute the processes of:

5 creating an encryption key out of a given piece of personal
6 identification information;

7 encrypting the personal identification information by use of the
8 encryption key and thereby recording the encrypted personal
9 identification information in the magnetic disk as verification data;

10 executing user verification based on the verification data
11 recorded in the magnetic disk; and

12 executing any of encrypting write data transmitted from a host
13 system by use of the encryption key and thereby recording the encrypted
14 write data in the magnetic disk, and decrypting the data read out of
15 the magnetic disk by use of the encryption key and thereby transmitting
16 the decrypted data to the host system.

1 Claim 23. (currently amended) A program stored in computer
2 readable memory for controlling a computer to control data writing and
3 reading in and out of a magnetic disk, the program causing the computer
4 to execute the processes of:

5 creating an verification encryption key out of a given piece of
6 personal identification information;

7 encrypting the personal identification information by use of the
8 verification encryption key and recording the encrypted personal
9 identification information in the magnetic disk as verification data,
10 and further encrypting a data encryption key by use of the verification
11 encryption key and thereby recording the encrypted data encryption key
12 in the magnetic disk;

13 executing user verification based on the verification data
14 recorded in the magnetic disk;

15 decrypting the data encryption key recorded in the magnetic disk
16 by use of the verification encryption key; and

17 executing any of encrypting write data transmitted from a host
18 system by use of the decrypted data encryption key and thereby

19 recording the encrypted write data in the magnetic disk, and decrypting
20 the data read out of the magnetic disk by use of the data encryption
21 key and thereby transmitting the decrypted data to the host system.

1 Claim 24. (new) The hard disk device according to claim 7,
2 wherein the control mechanism writes the data in the recording
3 medium without encrypting the data when the encryption function is
4 turned off.

1 Claim 25. (new) The data processing method of claim 17, wherein
2 the user verification comprises:

3 creating a candidate encryption key out of a given piece of
4 candidate personal identification information;

5 creating candidate verification data by encrypting the candidate
6 personal identification information by use of the candidate encryption
7 key; and

8 determining whether the candidate verification data are identical
9 to the verification data previously recorded in the recording medium.